

7/20/17
UNSEALED PER ORDER OF COURT

SEAL
UNITED STATES DISTRICT COURT

for the
Southern District of California

FILED
AUG 17 2016
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

Case No.

16MJ2530

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Facebook Inc, 1601 Willow Road, Menlo Park, CA)
For Records to Facebook User ID:)
<https://facebook.com/profile.php?id=100008589613118>)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe property to be searched and give its location): see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 912, and the application is based on these facts: See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Stirling Campbell, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/17/16


Judge's signature

City and state: San Diego, CA

Mitchell D. Dembin, United States Magistrate Judge
Printed name and title

du!

X673T
08/16/16**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Special Agent Stirling Campbell, upon being duly sworn do hereby state that the following is true to my knowledge and belief:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI) having been so employed since April 2006. I am currently assigned to the Special Agent in Charge (SAC) San Diego Office, Cyber Crimes Group within HSI in San Diego, California. Prior to this time, I worked as a United States Customs and Border Protection Officer in Los Angeles and Long Beach, California for approximately two (2) years and two (2) months. I have a Bachelor's Degree in Economics from the University of California, San Diego. I have assisted in the service of numerous search warrants involving computer/cyber-crimes. I am currently assigned to the Internet Crimes Against Children (ICAC) task force in San Diego, California. This task force includes members of the San Diego Police Department, San Diego County Sheriff's Department, U.S. Postal Inspection Service, Federal Bureau of Investigations, Naval Criminal Investigative Service, U.S. Attorney's Office and the San Diego County District Attorney's Office. Throughout my tenure with HSI, I have participated in numerous investigations involving child exploitation, human trafficking, human smuggling, financial crimes and narcotics. As an HSI Special Agent assigned to the ICAC task force, I investigate criminal violations relating to child exploitation, child pornography and cybercrimes, including violations pertaining to wire fraud and conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349, impersonating an officer, in violation of Title 18, United States Code, Section 912, blackmail, in violation of Title 18, United States Code, Section 873, extortion through interstate communications, in violation of Title 18, United States Code, Section 875, receiving proceeds of extortion, in violation of Title 18, United States Code,

1 Section 880, money laundering, in violation of Title 18, United States Code,
2 Sections 1956(a)(1)(A) and 1956(a)(3)(A), and conspiracy to commit these
3 offenses, in violation of Title 18, United States Code, Section 371. As a federal
4 agent, I am authorized to investigate violations of laws of the United States and I
5 am a law enforcement officer with the authority to execute warrants issued under
6 the authority of the United States. In preparing this affidavit, I have discussed the
7 facts of this case with other law enforcement agents, including officers within HSI
8 and the Office of Professional Responsibility (OPR).

9
10 2. This affidavit is made in support of an application for a warrant to search for
11 and seize evidence related to potential violations of Title 18, United States Code,
12 Sections 1343, 1349, 1956, 912, 873, 875, 876, 880 and 371, at the location
13 described in Attachments A, for evidence described in Attachment B.

14
15 3. This affidavit is based upon information I have gained through training and
16 experience, as well as upon information relayed to me by other individuals,
17 including law enforcement officers. Since this affidavit is being submitted for the
18 limited purpose of securing a search warrant, I have not included each and every
19 fact known to me concerning this investigation but have set forth only the facts
20 that I believe are necessary to establish probable cause to believe that evidence
21 relating to potential violations of Title 18, United States Code, Sections 1343,
22 1349, 1956, 912, 873, 875, 876, 880 and 371, described in Attachment B, is
23 located at Attachments A.

24
25
26 4. Based upon the following information, I believe there is probable cause to
27 believe that currently located within Attachments A there is evidence concerning
28
29

1 potential violations of Title 18 U.S.C. Sections 1343, 1349, 1956, 912, 873, 875,
2 876, 880 and 371, more particularly described in Attachment B.

3 4 **BACKGROUND ON FACEBOOK**

5
6 5. Facebook is a corporation that provides an online social networking service
7 and is headquartered in Menlo Park, California. After registering to use the site,
8 users can create a "page," to include a profile, adding others users as "friends,"
9 exchanging messages, posting status updates and photos, sharing videos, using
10 various applications and receiving notifications when others update their profiles.

11
12
13 6. A user can limit the access to his Facebook page. For example, the user can
14 adjust the settings on his page, so that the information he posts can be viewed by
15 the general public, or by a limited number of friends, or by just one individual.

16
17 7. Use of Facebook can generate IP addresses and/or GPS data.

18 19 **INVESTIGATIVE RESULTS**

20 21 **The Fraudulent Scheme**

22
23 8. On or about August 17, 2015, the Joint Intake Center (JIC) received a
24 complaint from an individual (hereafter referred to as V1). V1 stated he was
25 contacted by an agent from HSI's Cyber Crime Center (C3)¹ in order to extort

26
27
28 ¹ The Cyber Crimes Center (C3) is a legitimate section under HSI. It is comprised of the Cyber
29 Crimes Unit, Child Exploitation Investigations Unit, and Computer Forensics Unit. HSI's C3

1 money from him. V1 stated the agent identified himself as "Charles ROBERTS"¹
2 and demanded five hundred dollars (\$500) to forestall a pending arrest warrant for
3 V1. V1 sent \$500 per ROBERTS' instructions via MoneyGram Reference
4 Number 99283061. V1 said ROBERTS used the phone number (407) 731-7186.
5

6 9. On November 24, 2015, SSA Grundy and I interviewed V1. V1 stated that
7 during the month of July or August, 2015, he corresponded over email with a
8 person that he believed to be an adult female. He met this person through
9 Craigslist, a classified advertisements website, which includes personals.
10

11
12 10. V1 stated that approximately two (2) days after his communications with
13 this woman he received a call from "911." When V1 answered, a male identified
14 himself as "Charles ROBERTS," an agent assigned to the "C3 Child Exploitation
15 Division" in Florida. ROBERTS accused V1 of soliciting a minor on Craigslist
16 and viewing a photo of the alleged minor. ROBERTS claimed that he had an
17 arrest warrant for V1 as a result of this violation. ROBERTS then detailed
18 specifics about V1's employment. (V1 later deduced that ROBERTS likely gained
19 knowledge of his employment by querying V1's phone number, which was linked
20 to V1's professional profile on the website LinkedIn.)
21
22
23

24
25 delivers computer-based technical services to support domestic and international investigations
26 into cross border crimes and provides training to federal state, local and international law
27 enforcement agencies.

28 ¹ Senior Special Agent (SSA) James Grundy and I have conducted searches within HSI and
29 nowhere is an individual named "Charles Roberts" listed as an agent.

11. ROBERTS told V1 that since it appeared V1 had not been in trouble for prior violations, ROBERTS would speak with a C3 supervisor to allow V1's warrant to be cleared if V1 promptly paid a five hundred dollar (\$500) fine. ROBERTS emailed a copy of a "Warrant Purge" document to V1 reflecting what would be filed to nullify the warrant if the fine was paid. V1 recalled ROBERTS used a Gmail account with the words "c3" and "child exploitation" in the address. V1 stated the "Warrant Purge" displayed the DHS seal, a judge's name, legal jargon related to child exploitation and represented ROBERTS as an officer from the "C3."

12. ROBERTS directed V1 to a nearby Walmart and told V1 to use MoneyGram to send the \$500 payment, since MoneyGram was backed by the federal government and equipped to send ROBERTS a secure payment. V1 completed the money transfer per ROBERTS' instruction. V1 stated after he paid the fine, he then took a closer look at the "Warrant Purge" and realized there were spelling errors in the document and that it probably was a fake. V1 stated ROBERTS again tried to contact him to pay additional fines. V1 subsequently made the report of the extortion.

13. On November 24, 2015, V1 provided SSA Grundy and me a copy of an email he received from ROBERTS on Saturday, August 1, 2015, at 10:47 a.m. Pacific Standard Time (PST). ROBERTS used the email address **c3childexploitaiondivision@gmail.com** [sic] to send a document to V1. The document is titled "Warrant Purge" and reflects a payment of \$500. In summary, the "Warrant Purge" contains a DHS seal and the heading "IN THE DISTRICT COURT OF JUSTICE OF THE STATE OF California FIFTH DISTRICT."

1 Within the body of the document, the investigating agent is identified as “detective
2 CHARLES ROBERTS EMPLOYED AND SWORN IN UNDER THE C3 CHILD
3 EXPLOITATION UNIT.”

4
5 14. On December 11, 2015, I submitted a DHS Summons to Google, Inc.,
6 requesting all information associated to **c3childexploitaiondivision@gmail.com**.

7
8 15. On or about December 15, 2015, Google responded to the DHS Summons
9 and provided one file pertaining to Google account-holder(s) identified as
10 **c3childexploitaiondivision@gmail.com**. The following information was
11 provided by Google:
12

13 Name: Charles Roberts
14 e-Mail: **c3childexploitaiondivision@gmail.com**
15 Services: Gmail, Google Talk, Web History
16 Created on: 2015/07/26-20:50:56-UTC
17 Terms of Service IP: 64.45.224.30, on 2015/07/26-20:50:56-UTC
18 Google Account ID: 482292487891

19 Service remained ongoing through at least December 15, 2015.

20 16. On February 16, 2016, SSA Grundy and I interviewed an additional victim
21 (hereafter referred to as V2). V2 stated that he had been on the personals section
22 of Craigslist in July or August 2015. V2 gave an account similar to V1 about how
23 he initially began communicating with a person he believed to be an adult female.
24 He was then contacted by ROBERTS. ROBERTS identified himself as an agent
25 with HSI's C3 and accused V2 of soliciting a minor.
26
27
28
29

1 17. V2 confirmed he had also spoken with ROBERTS on phone number (407)
2 731-7186 during the month of July/August. This is the same number Roberts used
3 to call V1 in July/August 2015.

4
5 18. V2 stated that ROBERTS has changed his phone number several times after
6 their initial phone conversation. V2 stated approximately thirty (30) minutes
7 before meeting with SSA Grundy and me on February 16, 2016, he had spoken to
8 ROBERTS. At that time, ROBERTS was using the phone number (407) 613-
9 9452. ROBERTS continued to identify himself as a Special Agent with Homeland
10 Security and wanted to be apprised if any other Federal Law Enforcement
11 Agencies were to ever speak with V2 concerning his (ROBERTS') investigation.
12

13
14 19. During the interview, V2 provided SSA Grundy and me with an email that
15 he received from ROBERTS on August 22, 2015, at 8:40 a.m. PST. Attached to
16 the email was a document titled "Warrant Purge." The document is similar to the
17 previously described "Warrant Purge" document that was sent to V1, although this
18 Warrant Purge contains V2's name, and it was sent to V2 under a new email
19 address, **cybercrimescenter3@gmail.com**.
20

21
22 20. V2 stated he also sent monetary transactions in the forms of Homeland
23 Security "fees" and "fines" via MoneyGram to ROBERTS at ROBERTS' request.
24 Summons results from MoneyGram confirm multiple transactions sent by V2 to
25 ROBERTS and picked up at a Walmart in Kissimmee, Florida. (Open records
26 checks reflect the area code (407) used by the two (2) previously-mentioned phone
27 numbers used by ROBERTS include Orange, Osceola, and Seminole counties.
28 Kissimmee is located in Osceola County, Florida.)
29

The Connection to the Facebook Account

21. On August 24, 2015, V2 sent \$600 to ROBERTS as payment towards purging the outstanding warrant. MoneyGram summons results reflect that ROBERTS picked up the funds from a Kissimmee Walmart on August 25, 2015.

22. On August 26, 2015, an individual identified as Ronnie MONTGOMERY posted a self-produced video to **Facebook account profile** [https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118) of him picking up \$600 at a Walmart in-store MoneyCenter. This video was available to the general public from this Facebook account page. MONTGOMERY speaks throughout the video, and his voice can be distinctly heard.

23. In the opening scene of the video, the camera points at the teller's torso and hands at the Walmart, and Montgomery can be heard saying: "This is basically like another day at the office for a [UI], you know? He then tells the teller, "I done seen you so many times, I might as well just invite you over for Thanksgiving." The teller laughs. He adds, "I done came here and take all your twenties in the last couple 'a weeks." She answers, "uh-huh [yes]." While the teller types into a computer, Montgomery says, "The fruits of my labor, I enjoy it while it's still ripe." And "I love makin' money." As the teller counts out a wad of cash in front of Montgomery, he can be heard to say, "Okay.... That's all for me? ... Aww, you Santa Claus.... I love her." As he collects the money, Montgomery tells the teller, "Ohhh, look at that. You a sweetheart. You have a good one miss." Montgomery then aims the camera at himself and says, "Get money bitches."

1 24. On February 18, 2016, V1 and V2 both identified MONTGOMERY's voice
2 played from the video posted to **Facebook account profile**
3 **[https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)** as the individual they
4 spoke with over the phone known to them as ROBERTS.

5
6 25. On March 3, 2016, United States Magistrate Judge Karen Crawford of the
7 Southern District of California signed federal search warrants for **Facebook**
8 **account profile [https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)**. See
9 16MJ0621.

10
11
12 26. On or about March 17, 2016, I received search warrant results from
13 Facebook regarding **Facebook account profile [https://facebook.com/](https://facebook.com/profile.php?id=100008589613118)**
14 **[profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)**. Contained in the search warrant results were
15 private messages sent by MONTGOMERY to other individuals concerning his
16 involvement in criminal activity. For example, MONTGOMERY had the
17 following conversation with another individual identified as "WR" on January 23,
18 2016:

19
20 MONTGOMERY: Yeah I got another lick¹ I be doing works real good I'm
21 in Poinciana² now

22 WR: What kinda lick

23
24 MONTGOMERY: Cyber crime center

25 WR: Wtf is that
26

27
28 ¹ The term "lick" is slang for stealing from someone.

29 ² Poinciana is in Osceola and Polk Counties, Florida.

1 MONTGOMERY: Some crazy shut brother I make 3500 a week minimum
2
3

4 27. On April 19, 2016, V2 made a consensual monitored call to ROBERTS. V2
5 discussed with ROBERTS details about an upcoming required payment and
6 emotional difficulties he was having with his family due to the large financial
7 payouts required by ROBERTS. During the conversation, ROBERTS handed the
8 phone to a different individual who in turn identified himself as a DHS
9 psychologist.
10

11
12 28. The individual posing as the DHS psychologist directed V2 to tell his family
13 that he had a child overseas and the payments he had been making over the past
14 year were in support of the child he had fathered. V2 inquired what he should do
15 if members of his real family were to ask for pictures of the child. ROBERTS
16 retrieved the phone from the psychologist and told V2 that he (ROBERTS) would
17 provide V2 pictures of a woman and her child.
18

19
20 29. Later on that same day, V2 received pictures of a female and a toddler from
21 ROBERTS. Also on April 19, 2016, MONTGOMERY posted a link to a video of
22 the same toddler and female to **Facebook account profile**
23 **[https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)**. In addition to the
24 video, MONTGOMERY posted a comment, "It's a work thing don't ask."
25

26 30. On April 22, 2016, United States Magistrate Judge Barbara L. Major of the
27 Southern District of California signed a second search warrant for **Facebook**
28
29

1 **account profile [https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118). See**
2 **16MJ1174.**

3
4 31. On or about May 16, 2016, I received search warrant results from Facebook
5 regarding **Facebook account profile [https://facebook.com/profile.php?id=](https://facebook.com/profile.php?id=100008589613118)**
6 **100008589613118.** Contained in the search warrant results were private
7 messages sent by MONTGOMERY to other individuals concerning his
8 involvement in criminal activity. For example, MONTGOMERY had the
9 following conversation with another individual identified as "DJ" on April 6,
10 2016:

11
12 MONTGOMERY: HMU #MoneyMoves

13 DJ: Waddup

14 MONTGOMERY then sent an image of a United States District Court Arrest
15 Warrant. The warrant has "John Mack" listed as the defendant.

16
17 DJ: Macc gonna arrest himself? Lol

18
19 32. HSI agents identified John Mack as a known associate of
20 MONTGOMERY's, who has picked up funds related to the ongoing fraudulent
21 scheme on at least three occasions from a Walmart in Kissimmee, Florida.

22
23 33. From our investigation, it appears that MONTGOMERY continues to
24 perpetrate this fraudulent scheme.

25
26 34. In June 2016, HSI Orlando agents obtained a cellular phone tracking court
27 order from the Orange County Florida Circuit Court on one of the phone numbers
28 MONTGOMERY has used in his fraudulent scheme. During this time, HSI agents
29

1 observed that MONTGOMERY was transient, staying at multiple hotels during
2 the course of one week. The order was obtained to assist in the monitoring of
3 MONTGOMERY's movements. On August 4, 2016, the cellular tracking results
4 began to return a "Position Method Failure" location. Consequently, since August
5 4th, HSI agents have been unable to monitor MONTGOMERY's location through
6 the phone tracking mechanism.

7
8 35. On August 12, 2016, MONTGOMERY posted an image advertisement for
9 webzillavpn.com on the publically available part of his Facebook account profile
10 **<https://facebook.com/profile.php?id=100008589613118>**. The message under
11 the image states "Webzilla Unlimited Free VPN, Unblock any websites, Unblock
12 Apps & VoIP services, Surf the web anonymously, Secure any WiFi hotspot,
13 Protect your data & privacy." Montgomery is advertising for Webzilla, a company
14 which promises its users anonymous web surfing, the ability to unblock websites
15 and bypass firewalls, and "military grade" encryption of the users' data. See
16 www.webzillavpn.com. This action reflects not only that MONTGOMERY
17 appears to remain involved in fraudulent activity, but also that MONTGOMERY
18 is still using his Facebook page.

21 22 **PRIOR ATTEMPTS TO OBTAIN DATA**

23
24 36. On March 3, 2016, search warrant 16MJ0621 was obtained for Facebook
25 account profile **<https://facebook.com/profile.php?id=100008589613118>** for July
26 1, 2015, to March 3, 2016. On April 22, 2016, search warrant 16MJ1174 was
27 obtained for Facebook account profile **[https://facebook.com/](https://facebook.com/profile.php?id=100008589613118)**
28 **[profile.php?id=100008589613118](https://facebook.com/profile.php?id=100008589613118)** for March 3, 2016 to April 22, 2016. Recent
29

1 activity in August 2016 indicates that MONTGOMERY continues to use this
2 Facebook account in furtherance of his criminal activity and as a means of
3 communication.

4 5 **GENUINE RISKS OF DESTRUCTION**

6
7 37. Based upon my experience and training, and the experience and training of
8 other agents with whom I have communicated, electronically stored data can be
9 permanently deleted or modified by users possessing basic computer skills. In this
10 case, a preservation letter was sent to Facebook on or about February 24, 2016
11 ordering the preservation of data associated with the Facebook user ID
12 <https://facebook.com/profile.php?id=100008589613118>.
13

14 15 **FACEBOOK SERVICES AND INFORMATION**

16
17 38. Facebook owns and operates a free-access social networking website of the
18 same name that can be accessed at <http://www.facebook.com>. Facebook allows its
19 users to establish accounts with Facebook, and users can then use their accounts to
20 share written news, photographs, videos, and other information with other
21 Facebook users, and sometimes with the general public.
22

23
24 39. Facebook asks users to provide basic contact and personal identifying
25 information to Facebook, either during the registration process or thereafter. This
26 information may include the user's full name, birth date, gender, contact e-mail
27 addresses, Facebook passwords, Facebook security questions and answers (for
28 password retrieval), physical address (including city, state, and zip code),
29

1 telephone numbers, screen names, websites, and other personal identifiers.
2 Facebook also assigns a user identification number to each account.
3

4 40. Facebook users may join one or more groups or networks to connect and
5 interact with other users who are members of the same group or network.
6 Facebook assigns a group identification number to each group. A Facebook user
7 can also connect directly with individual Facebook users by sending each user a
8 "Friend Request." If the recipient of a "Friend Request" accepts the request, then
9 the two users will become "Friends" for purposes of Facebook and can exchange
10 communications or view information about each other. Each Facebook user's
11 account includes a list of that user's "Friends" and a "News Feed," which
12 highlights information about the user's "Friends," such as profile changes,
13 upcoming events, and birthdays.
14
15

16 41. Facebook users can select different levels of privacy for the
17 communications and information associated with their Facebook accounts. By
18 adjusting these privacy settings, a Facebook user can make information available
19 only to himself or herself, to particular Facebook users, or to anyone with access
20 to the Internet, including people who are not Facebook users. A Facebook user
21 can also create "lists" of Facebook friends to facilitate the application of these
22 privacy settings. Facebook accounts also include other account settings that users
23 can adjust to control, for example, the types of notifications they receive from
24 Facebook.
25
26

27 42. Facebook users can create profiles that include photographs, lists of
28 personal interests, and other information. Facebook users can also post "status"
29

1 updates about their whereabouts and actions, as well as links to videos,
2 photographs, articles, and other items available elsewhere on the Internet.
3 Facebook users can also post information about upcoming "events," such as social
4 occasions, by listing the event's time, location, host, and guest list. In addition,
5 Facebook users can "check in" to particular locations or add their geographic
6 locations to their Facebook posts, thereby revealing their geographic locations at
7 particular dates and times. A particular user's profile page also includes a "Wall,"
8 which is a space where the user and his or her "Friends" can post messages,
9 attachments, and links that will typically be visible to anyone who can view the
10 user's profile.
11

12
13 43. Facebook allows users to upload photos and videos, which may include any
14 metadata such as location that the user transmitted when s/he uploaded the photo
15 or video. It also provides users the ability to "tag" (i.e., label) other Facebook
16 users in a photo or video. When a user is tagged in a photo or video, he or she
17 receives a notification of the tag and a link to see the photo or video. For
18 Facebook's purposes, the photos and videos associated with a user's account will
19 include all photos and videos uploaded by that user that have not been deleted, as
20 well as all photos and videos uploaded by any user that have that user tagged in
21 them.
22

23
24 44. Facebook users can exchange private messages on Facebook with other
25 users. These messages, which are similar to e-mail messages, are sent to the
26 recipient's "Inbox" on Facebook, which also stores copies of messages sent by the
27 recipient, as well as other information. Facebook users can also post comments on
28 the Facebook profiles of other users or on their own profiles; such comments are
29

1 typically associated with a specific posting or item on the profile. In addition,
2 Facebook has a Chat feature that allows users to send and receive instant messages
3 through Facebook. These chat communications are stored in the chat history for
4 the account. Facebook also has a Video Calling feature, and although Facebook
5 does not record the calls themselves, it does keep records of the date of each call.
6

7 45. If a Facebook user does not want to interact with another user on Facebook,
8 the first user can “block” the second user from seeing his or her account.
9

10 46. Facebook has a “like” feature that allows users to give positive feedback or
11 connect to particular pages. Facebook users can “like” Facebook posts or updates,
12 as well as webpages or content on third-party (*i.e.*, non-Facebook) websites.
13 Facebook users can also become “fans” of particular Facebook pages.
14

15
16 47. Facebook has a search function that enables its users to search Facebook for
17 keywords, usernames, or pages, among other things.
18

19 48. Each Facebook account has an activity log, which is a list of the user’s posts
20 and other Facebook activities from the inception of the account to the present.
21 The activity log includes stories and photos that the user has been tagged in, as
22 well as connections made through the account, such as “liking” a Facebook page
23 or adding someone as a friend. The activity log is visible to the user but cannot be
24 viewed by people who visit the user’s Facebook page.
25
26
27
28
29

1 49. Facebook Notes is a blogging feature available to Facebook users, and it
2 enables users to write and post notes or personal web logs (“blogs”), or to import
3 their blogs from other services, such as Xanga, LiveJournal, and Blogger.

4
5 50. The Facebook Gifts feature allows users to send virtual “gifts” to their
6 friends that appear as icons on the recipient’s profile page. Gifts cost money to
7 purchase, and a personalized message can be attached to each gift. Facebook
8 users can also send each other “pokes,” which are free and simply result in a
9 notification to the recipient that he or she has been “poked” by the sender.
10

11
12 51. Facebook also has a Marketplace feature, which allows users to post free
13 classified ads. Users can post items for sale, housing, jobs, and other items on the
14 Marketplace.

15
16 52. In addition to the applications described above, Facebook also provides its
17 users with access to thousands of other applications (“apps”) on the Facebook
18 platform. When a Facebook user accesses or uses one of these applications, an
19 update about that the user’s access or use of that application may appear on the
20 user’s profile page.
21

22
23 53. Facebook uses the term “Neoprint” to describe an expanded view of a given
24 user profile. The “Neoprint” for a given user can include the following
25 information from the user’s profile: profile contact information; News Feed
26 information; status updates; links to videos, photographs, articles, and other items;
27 Notes; Wall postings; friend lists, including the friends’ Facebook user
28 identification numbers; groups and networks of which the user is a member,
29

1 including the groups' Facebook group identification numbers; future and past
2 event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and
3 information about the user's access and use of Facebook applications.

4
5 54. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP
6 address. These logs may contain information about the actions taken by the user
7 ID or IP address on Facebook, including information about the type of action, the
8 date and time of the action, and the user ID and IP address associated with the
9 action. For example, if a user views a Facebook profile, that user's IP log would
10 reflect the fact that the user viewed the profile, and would show when and from
11 what IP address the user did so.
12

13
14 55. Social networking providers like Facebook typically retain additional
15 information about their users' accounts, such as information about the length of
16 service (including start date), the types of service utilized, and the means and
17 source of any payments associated with the service (including any credit card or
18 bank account number). In some cases, Facebook users may communicate directly
19 with Facebook about issues relating to their accounts, such as technical problems,
20 billing inquiries, or complaints from other users. Social networking providers like
21 Facebook typically retain records about such communications, including records
22 of contacts between the user and the provider's support services, as well as records
23 of any actions taken by the provider or user as a result of the communications.
24

25
26 56. As explained herein, information stored in connection with a Facebook
27 account may provide crucial evidence of the "who, what, why, when, where, and
28 how" of the criminal conduct under investigation, thus enabling the United States
29

1 to establish and prove each element or alternatively, to exclude the innocent from
2 further suspicion.

3
4 57. In my training and experience, a Facebook user's "Neoprint," IP log, stored
5 electronic communications, and other data retained by Facebook, can indicate who
6 has used or controlled the Facebook account. This "user attribution" evidence is
7 analogous to the search for "indicia of occupancy" while executing a search
8 warrant at a residence. For example, profile contact information, private
9 messaging logs, status updates, and tagged photos (and the data associated with
10 the foregoing, such as date and time) may be evidence of who used or controlled
11 the Facebook account at a relevant time. Further, Facebook account activity can
12 show how and when the account was accessed or used. For example, as described
13 herein, Facebook logs the Internet Protocol (IP) addresses from which users access
14 their accounts along with the time and date. By determining the physical location
15 associated with the logged IP addresses, investigators can understand the
16 chronological and geographic context of the account access and use relating to the
17 crime under investigation. Such information allows investigators to understand
18 the geographic and chronological context of Facebook access, use, and events
19 relating to the crime under investigation. Additionally, Facebook builds geo-
20 location into some of its services. Geo-location allows, for example, users to "tag"
21 their location in posts and Facebook "friends" to locate each other. This
22 geographic and timeline information may tend to either inculcate or exculpate the
23 Facebook account owner. Third, Facebook account activity may provide relevant
24 insight into the Facebook account owner's state of mind as it relates to the
25 offenses under investigation. For example, information on the Facebook account
26 may indicate the owner's motive and intent to commit a crime (e.g., information
27
28
29

1 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting
2 account information in an effort to conceal evidence from law enforcement). Last,
3 Facebook account activity can assist in finding and confirming others'
4 involvement in the criminal offenses under investigation.

5
6 58. Therefore, the computers of Facebook are likely to contain the material
7 described above, including stored electronic communications and information
8 concerning the subscriber and his use of Facebook, such as account access
9 information, transaction information, and other account information.
10

11
12 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION**
13

14 59. Federal agents and investigative support personnel are trained and
15 experienced in identifying communications relevant to the crimes under
16 investigation. The personnel of Facebook are not. It would be inappropriate and
17 impractical for federal agents to search the vast computer network of Facebook for
18 the relevant accounts and then to analyze the contents of those accounts on the
19 premises of Facebook. The impact on Facebook's business would be severe.
20

21
22 60. I anticipate executing this warrant under the Electronic Communications
23 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A),
24 by using the warrant to require Facebook to disclose to the government copies of
25 the records and other information (including the content of communications)
26 particularly described in Section II of Attachment B. Upon receipt of the
27 information described in Section II of Attachment B, government-authorized
28
29

1 persons will review that information to locate the items described in Section III of
2 Attachment B.

3
4 61. Based on the foregoing, searching the recovered data for the information
5 subject to seizure pursuant to this warrant may require a range of data analysis
6 techniques and may take weeks or even months. Keywords need to be modified
7 continuously based upon the results obtained. The personnel conducting the
8 segregation and extraction of data will complete the analysis and provide the data
9 authorized by this warrant to the investigating team within ninety (90) days of
10 receipt of the data from the service provider, absent further application to this
11 court.
12

13
14 62. Based upon my experience and training, and the experience and training of
15 other agents with whom I have communicated, it is necessary to review and seize
16 all electronic communications that identify any users of the subject account(s) and
17 any electronic mails sent or received in temporal proximity to incriminating
18 electronic mails that provide context to the incriminating mails.
19

20
21 63. All forensic analysis of the imaged data will employ search protocols
22 directed exclusively to the identification, segregation and extraction of data within
23 the scope of this warrant.
24

25 **REQUEST FOR SEALING**
26

27 64. This is an ongoing investigation of which the target is unaware. It is very
28 likely, based upon the above, that evidence of the crimes under investigation exists
29

1 on electronic media subject to the control of the targets. There is reason to
2 believe, based on the above, that premature disclosure of the existence of the
3 warrant will result in destruction or tampering with that electronic media and
4 seriously jeopardize the success of the investigation. Accordingly, it is requested
5 that this warrant and its related materials be sealed until further order of the Court.
6 In addition, pursuant to Title 18, United States Code, Section 2705(b), it is
7 requested that this Court order the electronic service provider to whom this
8 warrant is directed not to notify anyone of the existence of this warrant, other than
9 its personnel essential to compliance with the execution of this warrant until
10 further order of the Court.
11

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

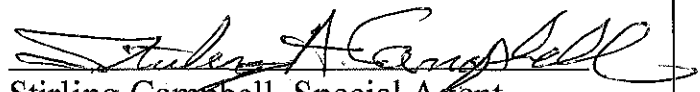
26 //

27 //

28 //

CONCLUSION

65. In conclusion, based upon the information contained in this affidavit, I have reason to believe that evidence, fruits and instrumentalities relating to violations of Title 18, United States Code, Sections 1343, 1349, 1956, 912, 873, 875, 876, 880 and 371, are located at the location described in Attachment A.


Stirling Campbell, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
this 17 day of August 2016.


THE HONORABLE MITCHELL D. DEMBIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

This warrant applies to information associated with the Facebook user ID **<https://facebook.com/profile.php?id=100008589613118>** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit Facebook, as custodian of the computer files described in Section II below, to locate the files relevant to attachment A and copy them onto removable electronic storage media and deliver the same to the officer or agent.

II. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A for the period of time from April 22, 2016, to August 16, 2016:

- a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos and videos uploaded by this user ID and all photos and videos uploaded by any user that have that user tagged in them;
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- f. All "check ins" and other location information;
- g. All IP logs, including all records of the IP addresses that logged into the account;
- h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- i. All information about the Facebook pages that the account is or was a "fan" of;
- j. All lists of friends created by the account;
- k. All records of Facebook searches performed by the account;
- l. All information about the user's access and use of Facebook Marketplace;
- m. The types of service utilized by the user;
- n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- p. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

1 III. Information to be seized by the government

2
3 All information described above in Section II that constitutes fruits, evidence and
4 instrumentalities of violations of Title 18, United States Code, Sections 912, 873,
5 875, 876, 880 and 371 involving Facebook user ID **[https://facebook.com/](https://facebook.com/profile.php?id=100008589613118)**
6 **[profile.php?id=100008589613118](https://facebook.com/profile.php?id=100008589613118)** from April 22, 2016 to August 16, 2016.
Specifically, information pertaining to the following matters:

- 7
- 8 a. Evidence pertaining to the assuming or pretending to be an officer or
9 employee acting under the authority of the United States or any
department, agency or officer thereof;
 - 10 b. Evidence indicating how and when the Facebook account was
11 accessed or used, to determine the chronological and geographic
12 context of account access, use, and events relating to the crimes under
investigation and to the Facebook account owner;
 - 13 c. Evidence indicating the Facebook account owner's state of mind --
14 including any references and/or admissions to the crimes under
15 investigation-- as it relates to the crimes under investigation;
 - 16 d. The identity of the person(s) who created or used the user ID,
17 including records that help reveal the whereabouts of such person(s);
 - 18 e. Evidence concerning the proceeds obtained from the fraudulent
19 activity discussed in the attached affidavit; and
 - 20 f. Evidence concerning any other individuals involved in the crimes
21 under investigation.
- 22
23
24
25
26
27
28
29